UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,165	09/30/2003	Ernie F. Brickell	42P16807	5908

8791 7590 07/26/2007
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/675,165	BRICKELL, ERNIE F.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) *1-12* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/2/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on May 02, 2007. Claims 1-19 are pending. Claims 1-12 are withdrawn by the applicant. At this time, claims 13-19 are rejected.

Election/Restrictions

2. Applicant's election without traverse of **species 2** in the reply filed on May 02, 2007 is acknowledged.

Claims 1-12 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected species 1, there being no allowable generic or linking claim. Election was made **without traverse** in the reply filed on May 02, 2007.

Information Disclosure Statement

3. The information disclosure statement (IDS) filed on May 02, 2007. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

4. Claim 13 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant and applicant's representative recite the phrase "using a fixed exponent ***substantially less*** in bit length than a bit length of a modulus (n)", wherein the word "substantially" is being indefinite. Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 13-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proudler et al (US 2003/0226031 A1), in view of Clapp (US 5,987,131), and further in view of Ober et al (US 6,959,086).

a. *Referring to claim 13:*

i. Proudler teaches a method comprising:

(1) receiving a request for information by a cryptographic device **(paragraphs 0065-0066 of Proudler);** and

(2) proving in a single direct proof that a value was signed by a signature key without revealing the value, the single direct proof comprises a plurality of exponentiations of which all of the plurality of exponentiations are conducted using a fixed exponent substantially less in bit length than a bit length of a modulus (n) **(paragraphs 0065-0066 of Proudler).**

ii. Although Proudler teaches a trusted device as shown in Figure 8 and paragraph 0037, Proudler is silent on the capability of using a direct proof, wherein an exponent having a bit length no more than one-half a bit length of a modulus (n) in his cryptographic information proving. On the other hand, Ober teaches:

(1) Selection of symmetrical key length is the second step (Block 4). The key management method supports several key lengths depending on the symmetrical block algorithm. The key length can be adjusted between the preferred range of about 40 bits and about 192 bits, depending on the PCDB programming. For a standard DES and Triple DES, keys can preferably have about a 40 bit to a about 192 bit key length, programmable in 8-bit increments by the application. This allows for variable key lengths other than the typical 40, 56, 112, and 192 bit key lengths found on the market. The third step (Block 6) of symmetrical key generation can preferably be performed six ways: 1) sample the output of a random number generator to assemble the desired length DEK; 2) sample the output of the random number generator to assemble the desired length KEK; 3) perform Diffie-Hellman g.sup.xy exponential in order to arrive at a shared secret value, such as based on ANSI X9.42; 4) derive a symmetrical secret key by hashing an application supplied password or passphrase; 5) transform a key using a combination of hashing, mixing

with fixed data and re-hashing, XORing, etc.; or 6) import a RED key provided by the application. The fourth step (Block 8) involves representing the secret key in one of preferably three ways: 1) inter-operable external form; 2) IRE (the encryption chip manufacturer) external form; or 3) IRE internal form. Numbers 2 and 3 are used to enforce the security policy, and Number 1 is used to allow shared key material with any other vendor's implementations. The symmetrical key inter-operable external representation step should be used when an application chooses to exchange the chip manufacturer's secret key with another crypto vendor. The secret key should be converted from the chip manufacturer's storage format into one that is more easily extractable so that it can inter-operate with other crypto vendors **(column 3, lines 22-57 of Ober).** In addition, Clapp teaches the direct proof in **column 2, lines 29-50 of Clapp**.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Proudler with the teachings of Ober for creating a trusted environment **(paragraph 0001 of Proudler).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Proudler with the teachings of Ober for Increasing the level of trust in platforms therefore enables greater user confidence that the platform and operating system environment behave in a known manner **(paragraph 0006 of Proudler).**

b. *Referring to claim 14:*

i. The combination of teaching between Proudler, Clapp, and Ober teaches the claimed subject matter. Clapp further teaches:

(1) wherein the bit length of the exponent being at most 160 bits in length **(column 2, line 45 of Clapp)].**

c. *Referring to claim 15:*

i. The combination of teaching between Proudler, Clapp, and Ober teaches the claimed subject matter. Ober further teaches:

(1) wherein the modulus (n) being over 1000 bits in length **[i.e., the modulus cannot be fixed, and a new modulus must be generated for each new public key pair (column 4, lines 25-26 of Ober). In addition, the modulus, public key and private keys can be exported/imported from/to the CryptIC. The public key is composed of two pieces: the public key (y) and the modulus data (p,q, and g). The CryptIC will allow a modulus size to be between 512 and 2048 bits with increments of 64 bits (column 17, lines 28-31 of Ober)].**

d *Referring to claim 16:*

i. The combination of teaching between Proudler, Clapp and Ober teaches the claimed subject matter. Ober further teaches:

(1) wherein the bit length of the fixed exponents associated with the exponentiations are a constant value despite any increase in value of the modulus (n) **[i.e., the key length can be adjusted between the preferred range of about 40 bits and about 192 bits, depending on the PCDB programming (column 3, lines 25-27 of Ober)].**

e: *Referring to claim 17:*

i. This claim has limitations that is similar to those of claim 13, thus it is rejected with the same rationale applied against claim 13 above.

ii. Proudler further teaches:

(1) a bus; a network interface card coupled to the bus; and a processor coupled to the bus **[i.e., as illustrated in Figure 2, the motherboard 20 of the trusted computing platform 10 includes (among other standard components) a main processor 21 with internal memory 25, main memory 22, a trusted device 24, a data bus 26 and respective control lines 27 and lines 28, BIOS memory 29 containing the BIOS program 28 for the platform 10 and an Input/Output (IO) device 23, which controls interaction between the components of the motherboard, the keyboard 14, the mouse 16 and the VDU 18. The main memory 22 is typically random access memory (RAM) (paragraph 0045 of Proudler)].**

f. *Referring to claim 18:*

i. This claim has limitations that is similar to those of claim 14, thus it is rejected with the same rationale applied against claim 14 above.

g. *Referring to claim 19:*

i. This claim has limitations that is similar to those of claim 16, thus it is rejected with the same rationale applied against claim 16 above.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Thanhnga B. Truong
AU2135

TBT
July 20, 2007